Improving Public Safety Wireless Communications and Interoperability

March 17, 2004

David Boyd, Director
Dereck Orr, Chief of Staff
SAFECOM@dhs.gov
Office: 202.772.9958

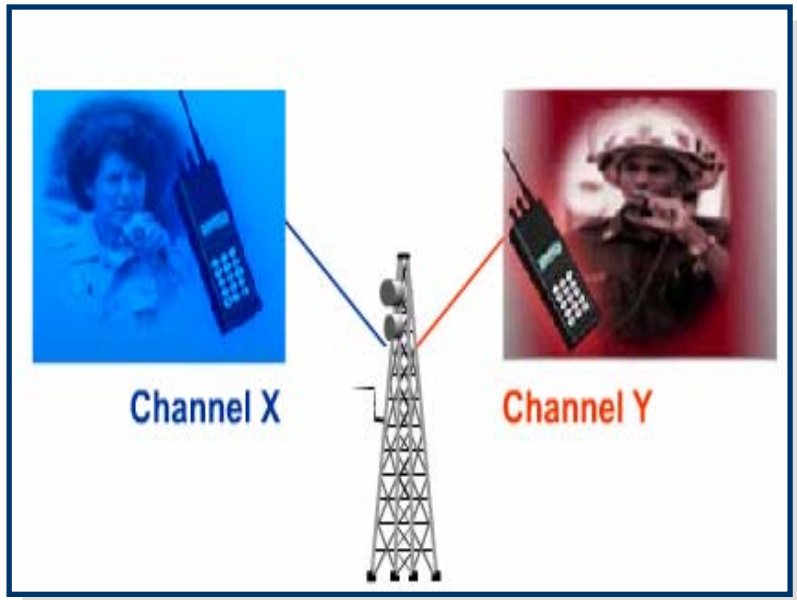
SAFECOM: Assuring a safer America through effective public safety communications

- Background on public safety communications and interoperability
- Major challenges to interoperability
- Role, vision, and objectives of SAFECOM
- Public Safety Communications Statement of Requirements
- Appendixes
  - A: Spectrum
  - B: Funding
  - C: Standards
  - D: Security

What is public safety wireless "interoperability"?

- **Wireless interoperability** is the ability of public safety service and support providers to talk with each other via voice and data
  - on demand
  - in real time
  - when needed
  - when authorized

- Wireless interoperability is necessary to—
  - Improve the ability of public safety officers to save lives and property
  - Facilitate rapid and efficient interaction among all public safety organizations
  - Provide immediate and coordinated assistance in day-to-day missions, task force operations, and mass-casualty incidents



Several high-profile events have underscored the critical importance of interoperability

1980

- Crash of Air Florida Flight 90, Washington, DC—January 13, 1982
  - "Stovepipe" public safety communications systems complicated on-scene, inter-agency communications
  - No provision for communications interoperability among the existing systems was in place
  - Sheer volume of calls exceeded system capacities

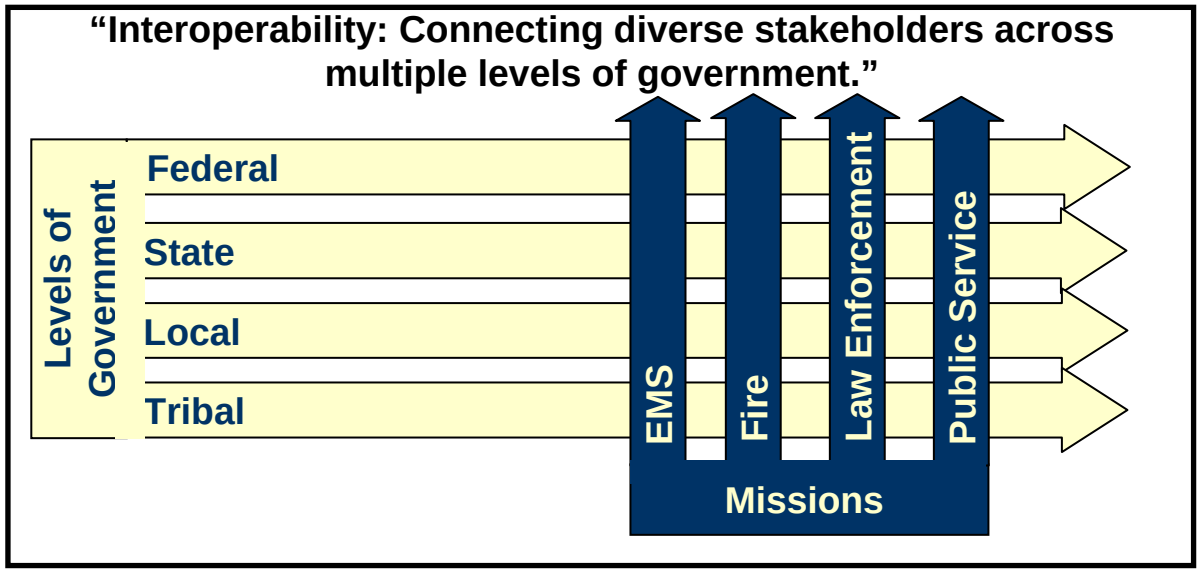
1990

- Alfred P. Murrah Building Bombing, Okalahoma City—April 19, 1995
  - In the aftermath of the attack, 117 local, state, and federal agencies responded with more than 1,500 personnel on the scene
  - Overwhelming call volume and disparate frequencies complicated emergency response
  - Responders were forced to rely on relay runners to disseminate critical, time-sensitive information

- World Trade Center Attack, New York City—September 11, 2001
  - After the south tower collapsed, police helicopters relayed a message for public safety officials to evacuate the north tower
  - Firefighters never received the police warning because their legacy radio systems malfunctioned and did not interoperate with the police communications systems

2003

Interoperability impacts a broad stakeholder base across missions and levels of government

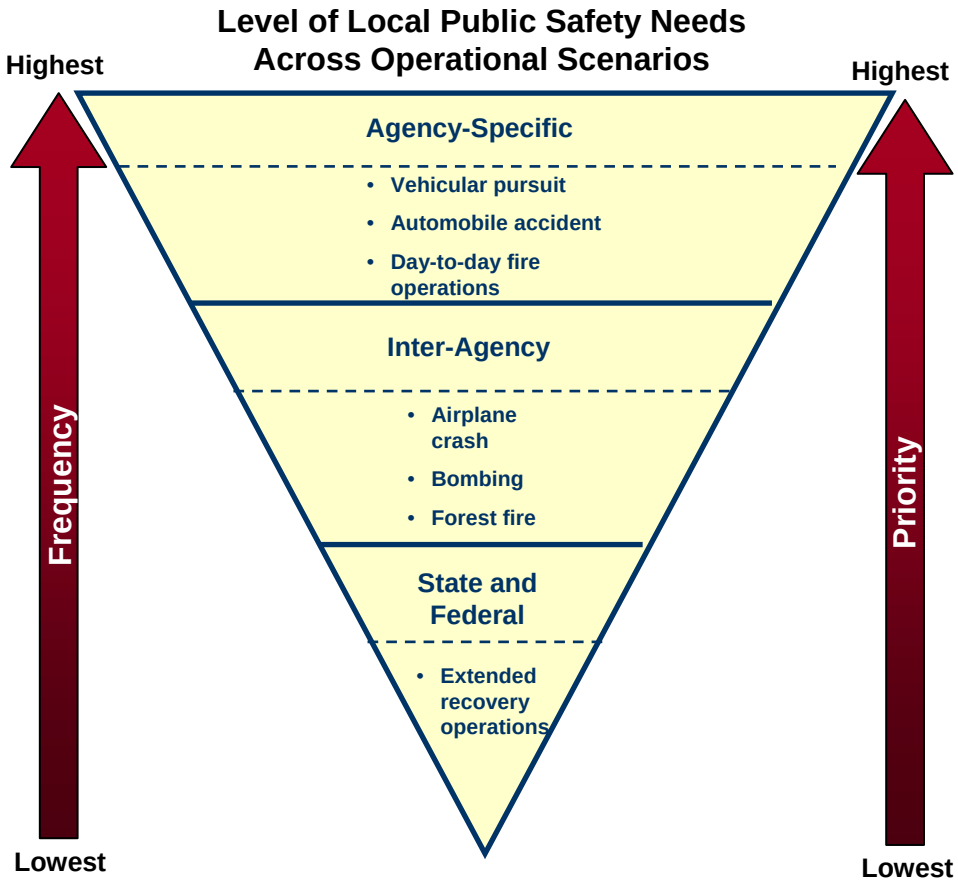


- Interoperability directly impacts the first responder community, which consists of over 61,000 public safety agencies including—
  - 960,000 Firefighters
  - 830,000 EMS Personnel
  - 710,000 Law Enforcement Officers
  - 28,495 Fire Departments [1]
  - 5,841 EMS Departments [1]
  - 27,496 Law Enforcement Agencies [1]
  - 25,763 Local Agencies [1]
  - 6,396 State Agencies [1]
  - 2,967 Federal Agencies [1]
- Interoperability also affects the public service arena, which includes legislative officials, utilities agencies, and chief information officers

[1] Source: www.SafetySource.com

The local public safety community is the practitioner of interoperability

- Local agencies are primarily concerned with communications within their own agency, but must work with other surrounding agencies
- The local public safety community's responsibilities range from—
  - Stabilizing the situation; to
  - Establishing initial communications links
- Local and state agencies own more than 90 percent of the existing public safety communications infrastructure
- A survey indicates that nearly one-third of local public safety agencies cite interoperability as inadequate



The Federal Government's role is to act as an enabler of interoperability

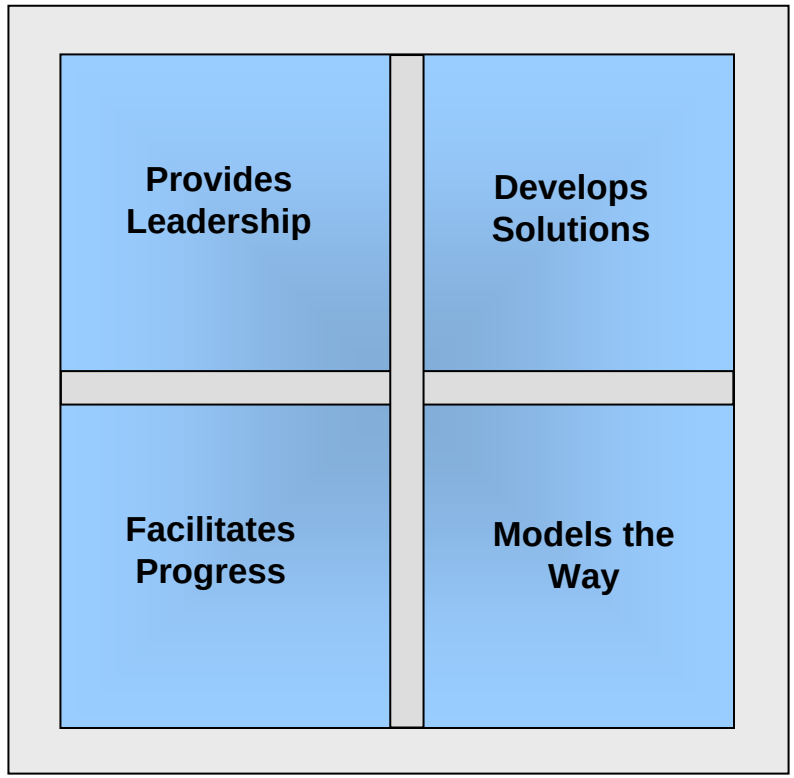
The Federal Government—

- Establishes a vision and charts a course for improvement
- Tests emerging technologies to identify innovative interoperability solutions
- Develops and promotes pilot systems to evaluate and promote solutions
- Builds collaborative relationships where federal agencies assist local and state agencies with solution implementation

Federal Government Constraints—

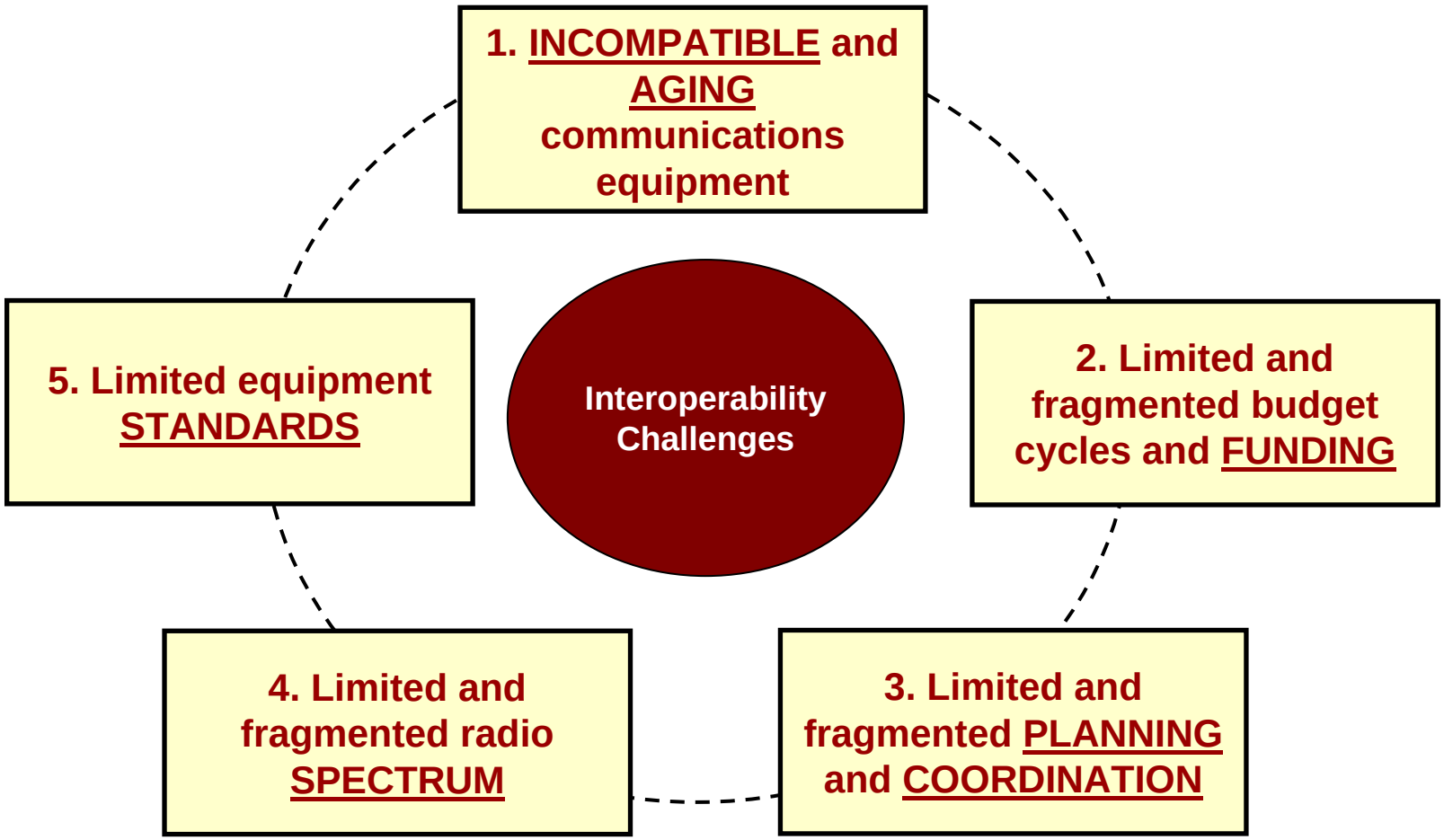
- Cannot single handedly fund interoperability improvements at all levels of government
- Cannot mandate that local and state agencies purchase new equipment to achieve interoperability

Roles of the Federal Government as an Enabler



- Background on public safety communications and interoperability
- **Major challenges to interoperability**
- Role, vision, and objectives of SAFECOM
- Public Safety Communications Statement of Requirements
- Appendixes
  - A: Spectrum
  - B: Funding
  - C: Standards
  - D: Security

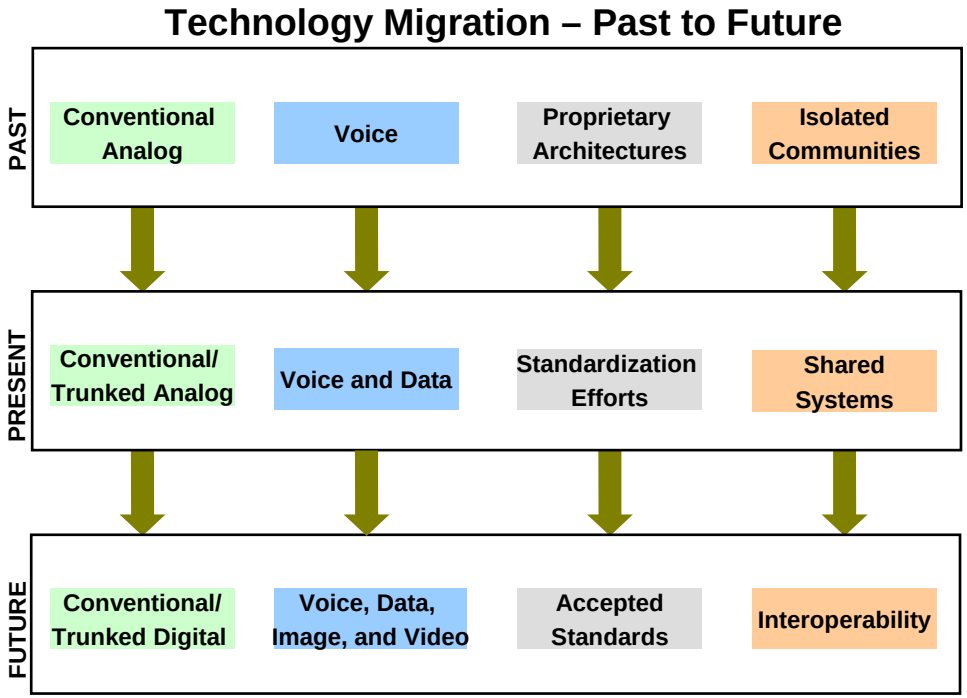
The complexity of the current state of interoperability is reflected in five key challenges



These five issues were identified by the National Task Force on Interoperability in its February 2003 final report, Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives.

Reason 1: Incompatible and aging communications equipment

- Public safety communications infrastructure and equipment is often in use well past its useful life
  - Outdated analog infrastructure exists in many jurisdictions
  - Many communications systems are up to 30 years old, rendering interoperability difficult
- Outdated equipment is unable to accommodate advanced features needed to support operations
- Agencies using equipment operating in disparate frequency bands cannot communicate with one another
- The use of proprietary technologies hinders the ability to interoperate with other agencies

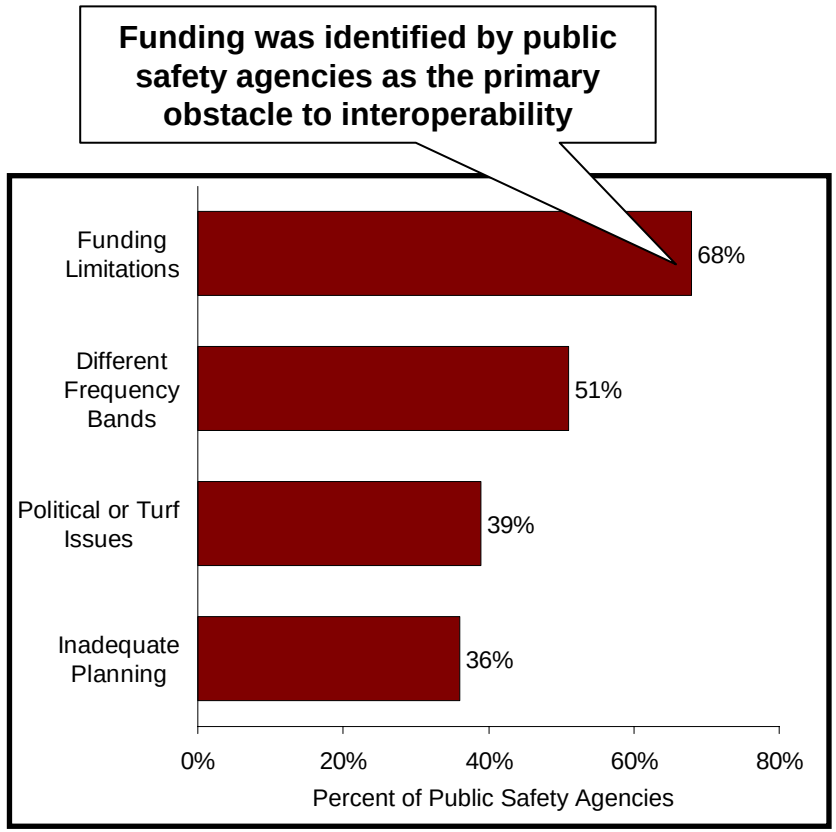


"We have 30-year systems being implemented in a 18-month technology cycle ."

- SAFECOM Strategy Planning Workshop participant, May 2003

Reason 2: Limited and fragmented budget cycles and funding

- Additional funding is needed to address interoperability
  - Existing infrastructure capital investment for local, state, and federal LMR systems have been estimated to be in excess of $18 billion
  - Replacement of LMR systems could reach $40 billion
  - Funding for wireless systems is in direct competition with other priorities
- Coordinated grant guidance is needed
  - Historically, many programs provided funding for communications equipment with different requirements and guidance
- Budget coordination is needed across levels of government
  - Local and state agencies have different acquisition requirements, planning cycles, and technical requirements
  - Traditionally, funding has been stove-piped to meet individual agency needs
  - Each agency may be in a different stage of technology replacement

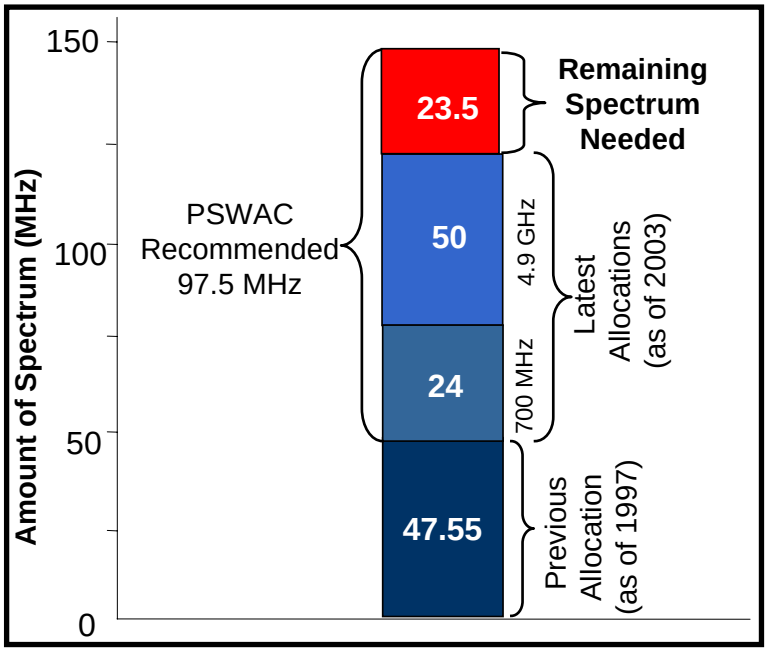


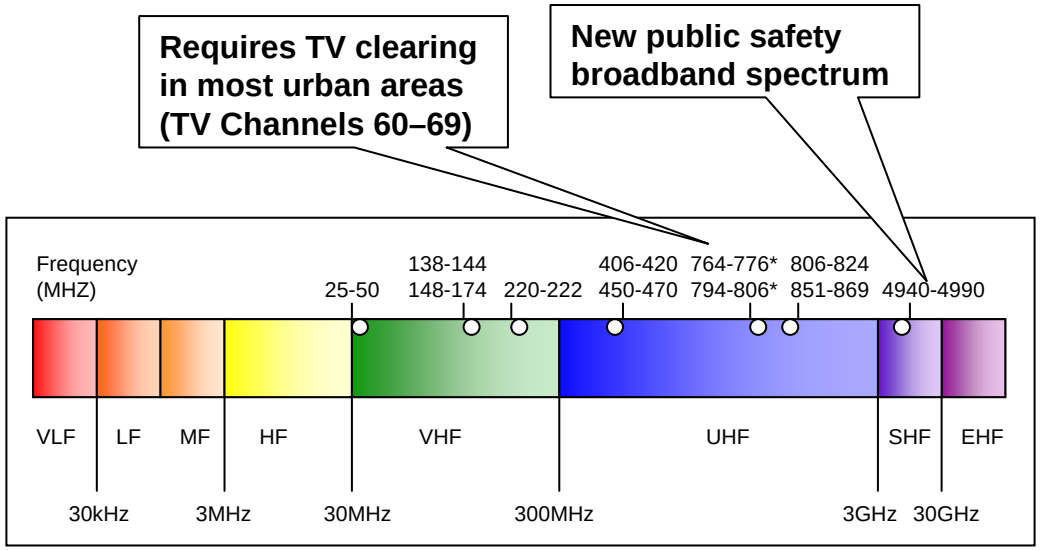
Source: Combined analysis of National Institute of Justice law enforcement and PSWN Program fire and EMS interoperability studies.

Reason 3: Limited and fragmented planning and cooperation

- Jurisdictional boundaries and unique missions often create barriers that hinder cooperation and collaboration
  - Many agencies are small, often volunteer organizations with limited budgets and little engineering expertise
  - No universal solution for every jurisdiction exists
- Financial and human factors that complicate interoperability planning include—
  - Lack of funding and resources
  - Management and control issues
  - Integration of policies and procedures
  - Cultural and operational differences among local, state, federal, and tribal agencies
- Interoperability is not sufficiently understood by decision makers or the organizations that influence those decision makers
- In the past, federal interoperability efforts were not coordinated effectively
  - Coordination among grant providers is needed to establish common grant criteria and requirements
  - Federal interagency communications has struggled due to a lack of coordination

Reason 4: Limited and fragmented radio spectrum





- The radio spectrum extends from 9 kHz to 300 GHz and is separated into more than 450 bands
  - Most public safety spectrum exists between 25 MHz and 800 MHz
- Spectrum available for public safety is limited and distributed across 10 disparate bands
- In 1996, the Public Safety Wireless Advisory Committee (PSWAC) estimated that an additional 97.5 MHz of radio spectrum would be needed to meet public safety communications requirements
  - Only 74 MHz has been allocated; however, none has been turned over for public safety use

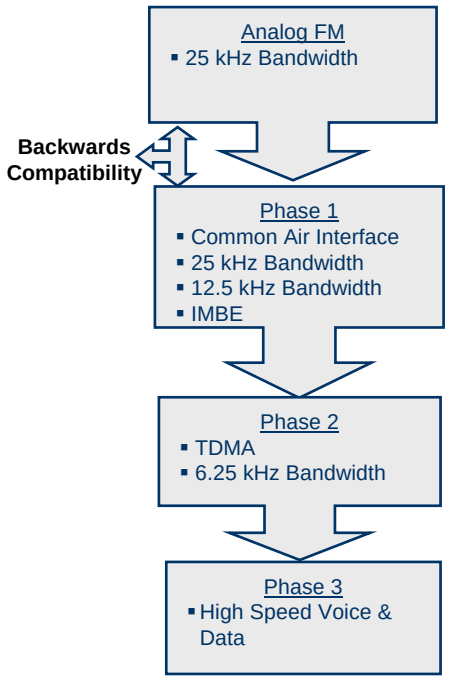
Reason 5: Limited equipment standards

Issues—

- The lack of a universally recognized, fully open, implementable standard for public safety has limited the cost efficiencies of interoperability
- Public safety has lagged behind the commercial sector in adopting new technology and open standards
- Development of proprietary protocols, resulting in equipment that is not interoperable
- Lack of competition in the land mobile radio (LMR) marketplace

Project 25—

- Steering committee, called Project 25 (P25), was formed by APCO, NASTD, and Federal Government agencies for selecting common digital system standards
- P25 has been segmented into three phases based on two underlying objectives—
  - **Improving interoperability** among first responders
  - **Introducing competition** into the LMR marketplace
- Output of P25 is a suite of standards and bulletins that outline equipment interoperability and compatibility requirements
- Advantages of P25 standards include—
  - Cost effective equipment upgrade and maintenance
  - Backwards compatibility
  - Improved interoperability
  - Increased competition in the LMR marketplace



Evolution of P25 Technical Specifications

Other key challenges that hinder interoperability include…

Inadequate Commercial Alternatives

- The commercial marketplace does not offer public safety grade voice services
- Little competition exists in the public safety equipment marketplace
- Commercial systems do not support one-to-many communications
- Priority access and/or dedicated services are not available to public safety

System Security Constraints

- Varying levels of security complicate efforts to integrate networks
- Network security vulnerabilities continue to increase rapidly due to the proliferation of new technologies
- Interoperability itself introduces security vulnerabilities
- Agencies are unfamiliar with new computer-based threats

Insufficient Understanding of Interoperability

- There is a general lack of awareness of the interoperability issue
- Decision makers have a limited understanding of the priority placed on interoperability
- There is uncertainty regarding the appropriate actions for addressing interoperability

- Background on public safety communications and interoperability
- Major challenges to interoperability
- **Role, vision, and objectives of SAFECOM**
- Public Safety Communications Statement of Requirements
- Appendixes
  - A: Spectrum
  - B: Funding
  - C: Standards
  - D: Security

SAFECOM was created to coordinate interoperability efforts across the Federal Government

SAFECOM serves as the umbrella program within the Federal Government to coordinate the efforts of local, state, federal, and tribal public safety agencies working to improve public safety response through more effective, efficient, interoperable wireless communications

- SAFECOM is one of the President's top three E-Government initiatives
- SAFECOM is a program driven by public safety practitioners
- Dedicated to develop better technologies and processes for the cross-jurisdictional and cross-disciplinary coordination of existing systems and future networks
- Responsible for outreach to local, state, and federal public safety agencies and to assist in interoperability planning and implementation

SAFECOM's efforts are funded by a number of federal partners

Department of Homeland Security

Department of Energy

Department of Health and Human Services

Department of Treasury

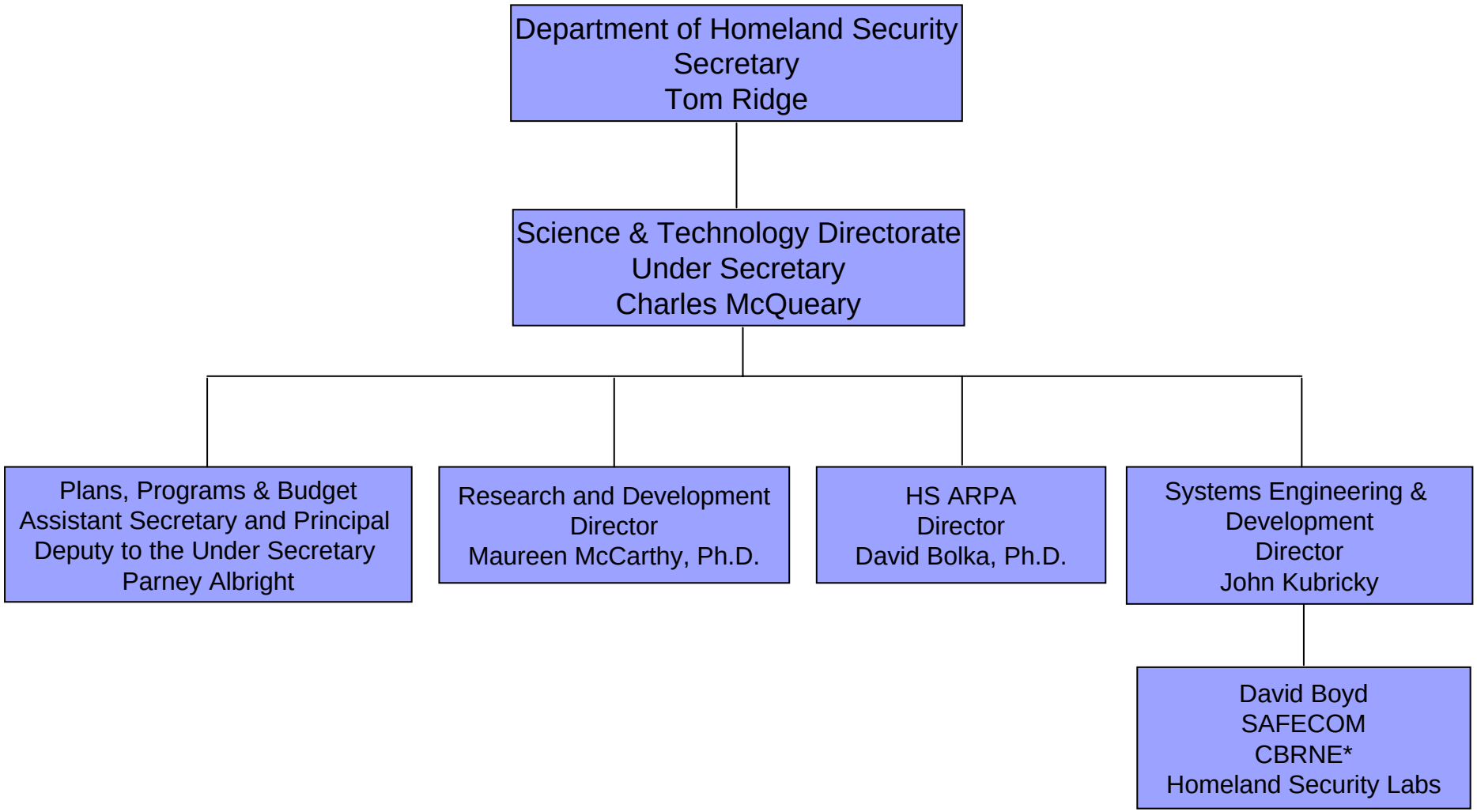
Department of Defense

Department of Interior

Department of Justice

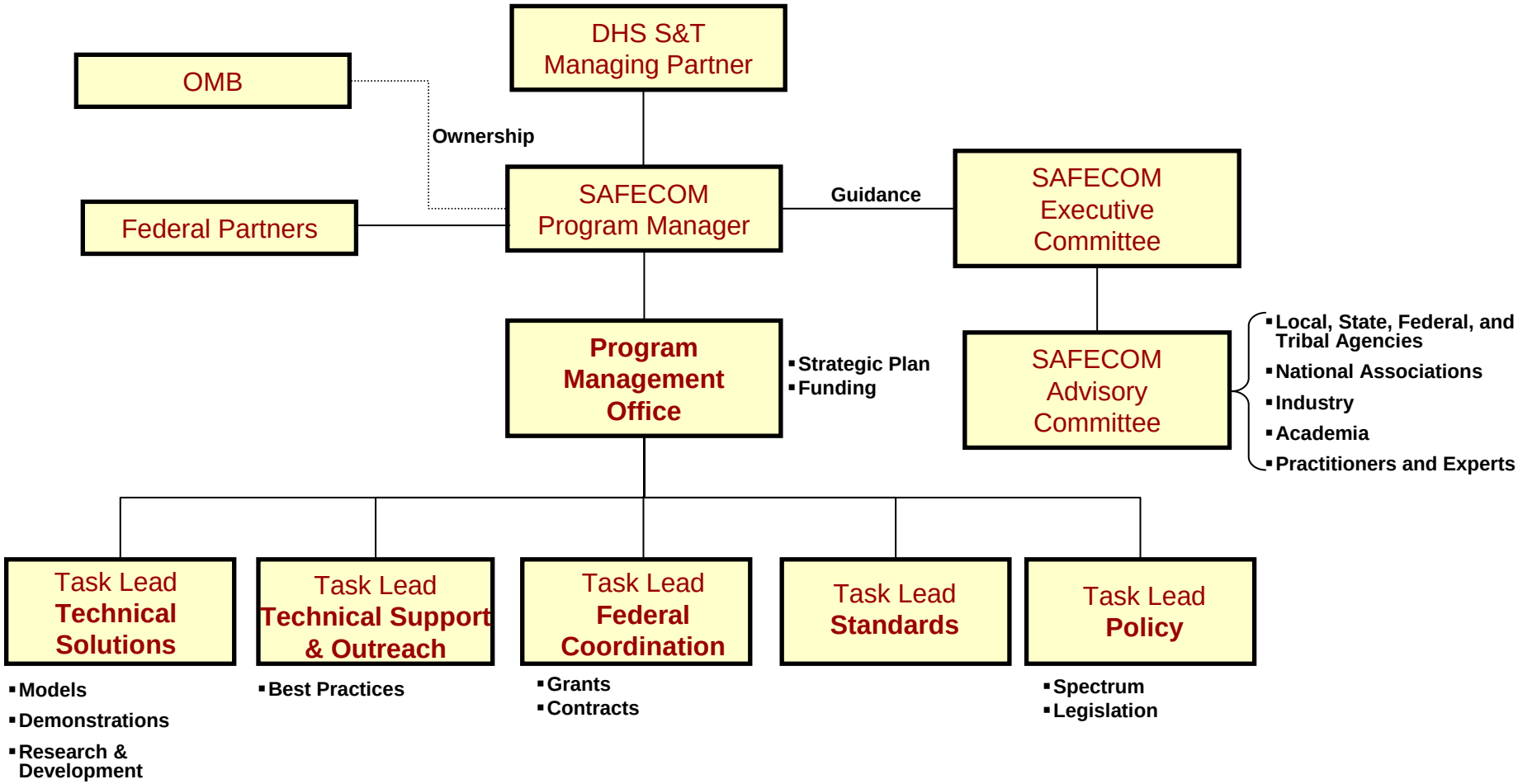
Department of Agriculture

SAFECOM is managed by the DHS Science and Technology Directorate



* Chemical, Biological, Radiological, Nuclear and Explosive

SAFECOM has established a governance structure to manage program operations



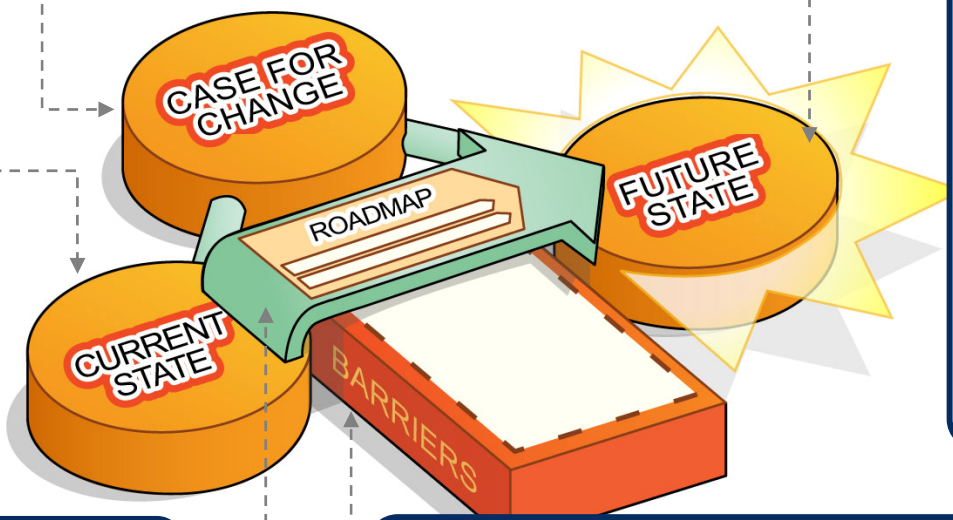
SAFECOM has developed a "roadmap" to help improve the state of interoperability

Current State

- Distrust among key players (local/state/federal)
- Short technology cycles vs. long operations lifecycles
- No standard, guidance, or national strategy for interoperability
- Fragmentation and limitations of the public safety spectrum
- No enforceability in federal grant use
- Vendor-driven environment
- No funding for training, planning, maintenance

Case for Change

- Avoid unnecessary loss of life and property
- Save money
- Facilitate sharing of resources across disciplines and jurisdiction
- Avoid delay, which makes the situation worse



Future State

- Public safety officers can transmit and receive all information (data/voice/video) necessary to maximize their effectiveness
- Public/private and local/state/federal partnerships
- Consistent, bankable source of funding for equipment, training, maintenance
- Vendors are driven by user requirements
- Ability to upgrade functions without purchasing new hardware

Roadmap

- Provide policy recommendations
- Develop a technical foundation
- Coordinate funding assistance
- Provide technical assistance

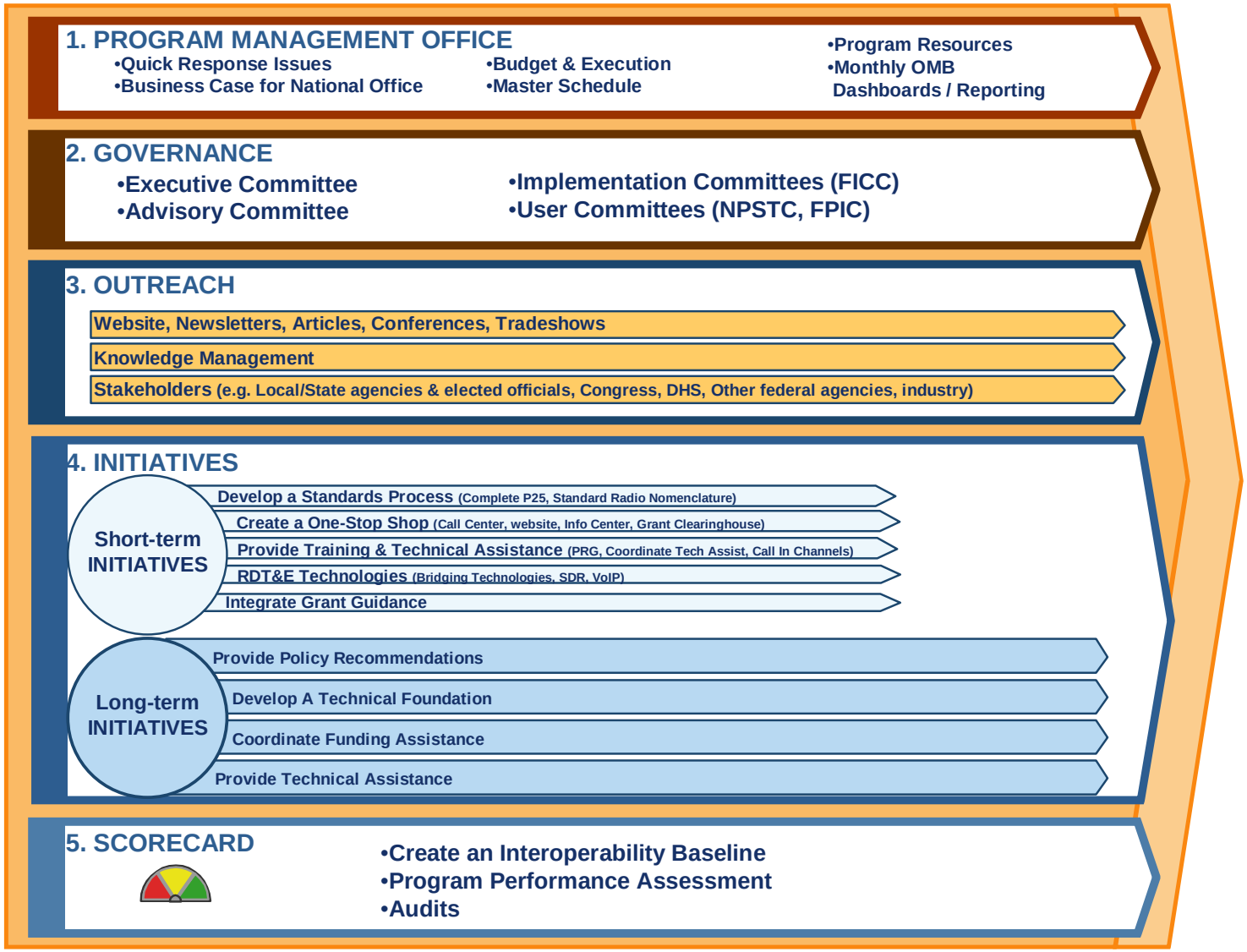
Barriers

- Insufficient funding for public safety communications infrastructure improvements
- Lack of staffing for SAFECOM program
- Local and state organizations' fear of federal mandates
- Limited credibility based on coordination efforts of federal agencies
- Inconsistency in the grants programs

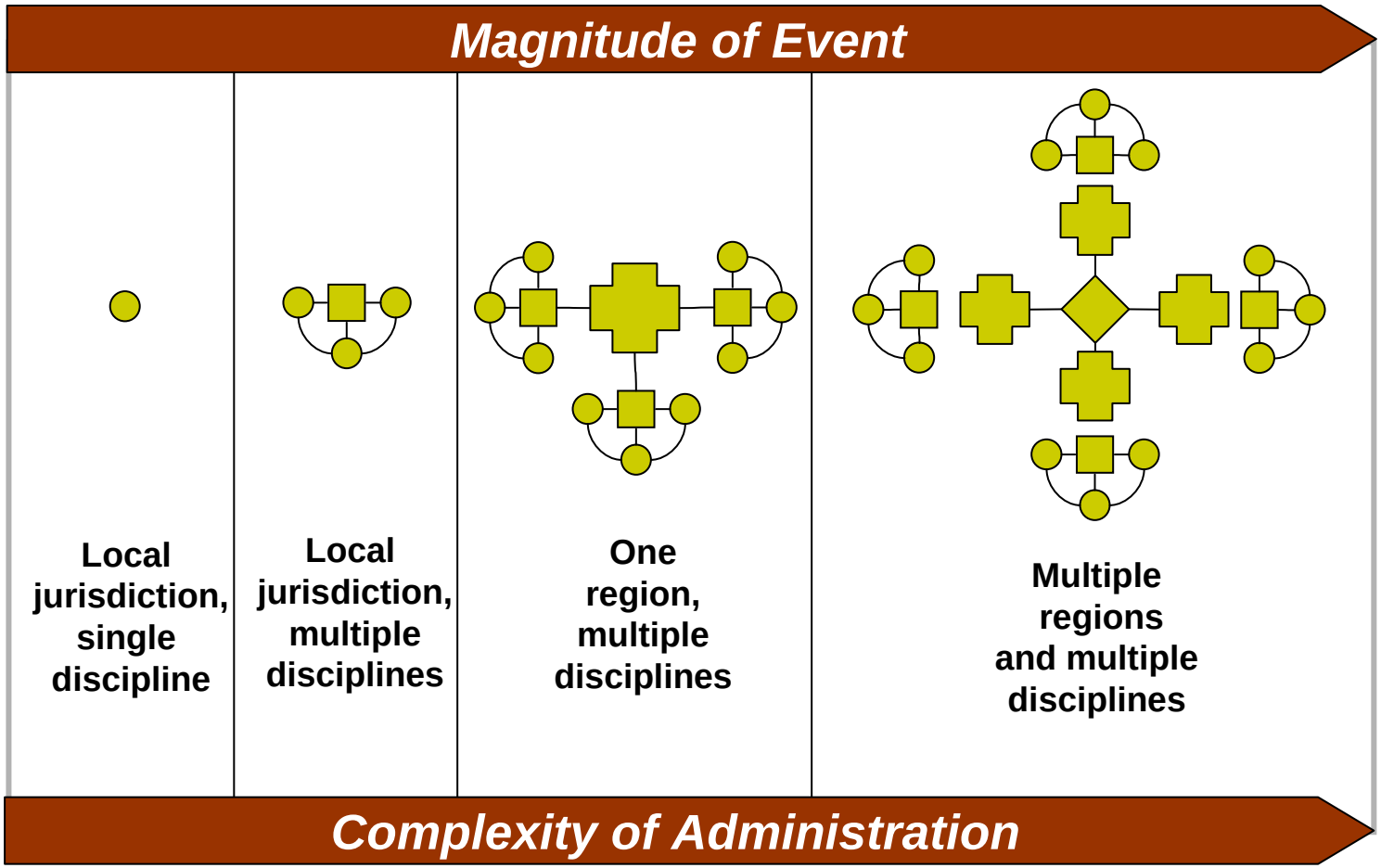
SAFECOM has developed a strategy to achieve necessary levels of interoperability

AS IS

TO BE



SAFECOM's long-term vision—a national "system of systems" that adapts to the incident



SAFECOM's long-term objectives…

- **Provide Policy Recommendations**
  - Represent public safety on the White House Spectrum Task Force
  - Inform the FCC and other federal agencies on the impact of their policies on local and state public safety agencies

- **Develop a Technical Foundation**
  - Research and Development
  - Fund demonstration projects of innovative technologies and solutions
  - Support the development of standards to achieve interoperability
  - Provide industry with public safety requirements and guidance

- **Coordinate Funding Assistance**
  - Tie federal funding assistance to grant guidance
  - Create a clearinghouse of interoperability information about grants, best practices, and equipment purchases

– **Provide Technical Assistance**
  - Develop and promote best practices for local and state agencies
  - Provide handbooks, publications and on-line information to assist local and state agencies
  - Provide technical support to local and state agencies in the implementation of communications systems

Over the next 18 months, SAFECOM has committed to…

- Create a baseline of public safety communications and interoperability
- Create a one-stop shop for public safety communications and interoperability
- Continue to integrate coordinated grant guidance across all grant making agencies
- Develop a process to advance standards
- Provide technical assistance for public safety communications and interoperability
- Develop tools to help jurisdictions build a business case to improve interoperability
- Research, develop, test & evaluate (RDT&E) existing & emerging technologies for improved public safety communications and interoperability

Objectives for 2008…

- All public safety agencies in the United States have a minimum level of interoperability, as defined by the national interoperability baseline
- Baseline plus 10% of public safety agencies in the United States are fully interoperable across disciplines at all levels of government
- Public safety interests, rather than vendors, drive communications and interoperability solutions and standards

Objective for 2023…

- There is an integrated system-of-systems, in regular use, that allows public safety personnel to communicate (voice, data, and video) with whom they need, on demand, in real time, as authorized.
  - Public safety can respond anywhere, bring their own equipment, and can work on any network immediately, when authorized
  - Public safety will have the networking and spectrum resources it needs to function properly

Overview of SAFECOM

Other Coordination Efforts

Interoperability Testing

Coordinate interoperability equipment and solutions testing
- AGILE
- NLECTC
- ITS

1. **Technical Solutions**
   - Pilot demonstrations
2. **Technical Support and Outreach**
   - Interoperability assistance
   - Case studies
   - Symposiums and conferences
   - Clearinghouse services
   - Web site
   - Awareness campaign
   - Informational materials
3. **Federal Coordination**
   - Integrate grant guidance across the Federal Govt
4. **Policy**
   - Spectrum monitoring
   - Legislation monitoring
   - Security studies
   - Funding studies
5. **Standards**
   - Project 25 support
   - Project MESA leadership

- Background on public safety communications and interoperability
- Major challenges to interoperability
- Role, vision, and objectives of SAFECOM
- **Public Safety Communications Statement of Requirements**
- Appendixes
  - A: Spectrum
  - B: Funding
  - C: Standards
  - D: Security

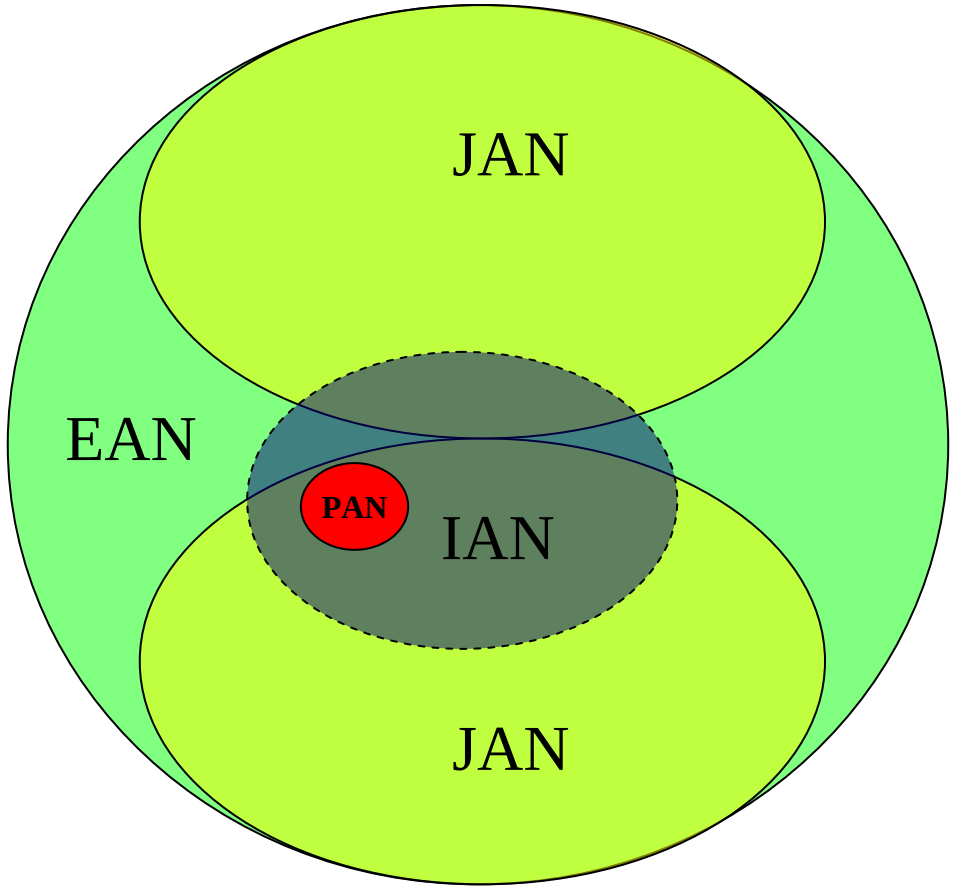
SAFECOM advocates the creation of a System of Systems architecture solution for interoperability.

The System of Systems involves interaction between the:

- Personal Area Network (PAN)
- Incident Area Network (IAN)
- Jurisdiction Area Network (JAN)
- Extended Area Network (EAN)

System Capabilities

- Practitioners seamlessly move between Jurisdictional Area Networks
- Practitioners join and leave networks as needed
- Allows for the creation and Growth of Temporary Networks
- System can recognize, register, authorize, and grant interoperable communications with the new resources



The System of Systems architecture builds from Personal Networks to Extended networks, and puts an emphasis on the individual public safety practitioner

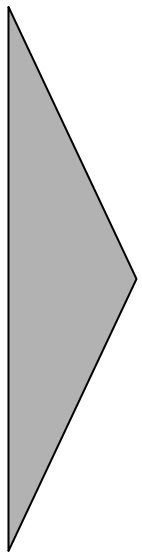
Different communications systems seamlessly integrate to form the various networks

The Purpose and Applications of the Public Safety Communications Statement of Requirements

- The purpose of this SoR is to identify a basic set of operational and functional communication requirements for public safety first responders to communicate and share information.
- Focus is initially on public safety first responders, i.e. Law Enforcement, Fire, EMS.
  - Future versions will engage other stakeholders, i.e. Tribal, Federal, supplemental responders, and other agencies

Basis

- Functional needs of public safety first responders
- Intended to be “blue sky” in nature, not limited to current implementations or technologies
- Leverage current “state-of-the-art” technology
- Not keyed to the issue of spectrum allocation
- Not tied to specific technology



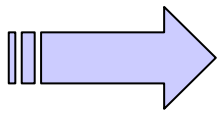
Applications

- Consolidate Public Service vision for policymakers and the public
- Drive Federal Assistance programs
- Prioritize R&D investment strategies
- Identify priorities for Field Test and Evaluation Plans.
- Identify priorities for Standards Development
- Creates the framework for discussion of operational issues

The Creation of the Public Safety Communications Statement of Requirements

- A SAFECOM document, jointly developed with support and assistance from the AGILE Program.
- Started as an SDR SoR. Evolved into a more comprehensive SoR

Vetting process involved technical subject matter experts public safety practitioners from all disciplines



Practitioners involved in the SoR Development

- National Association of State EMS Directors (NASEMSD)
- Charlottesville Fire Dept.
- City of Phoenix Fire Dept.
- Tualatin Valley Fire & Rescue
- Alexandria Police Dept.
- Arlington Police Dept.
- Madison County, NY Sheriff Dept.

The final SoR was reviewed and critiqued by the NPSTC Technical working group.

The Content of the Public Safety Communications Statement of Requirements

- Defines public safety roles and functions, including First Responders and Supplemental Responders
- Defines the required communications services for the first responders, i.e. voice, data, video
- Provides real-world implementation scenarios with a focus on future-looking communications
  - Includes operationally focused scenarios.
- Contains Operational Requirements for each discipline and Functional Requirements of the technology

Operational Requirements

Modes of Operation
- Day-to-Day/Routine
- Task Force
- Mutual Aid

Modes of Communication
- Interactive
- Non-Interactive

Operational Uses
- With Whom?
- For What Purpose?
- Special Constraints

Functional Requirements

Services
- Voice
- Data

Required Features
- Mobility
- Scalability
- COTS-based
- Backward Compatibility
- Open standards-based design
- Migration path for legacy systems
- Extensibility

Performance Requirements
- QoS
- Availability
- Reliability
- Survivability.

The Statement of Requirements will continue to evolve.

The SoR is a "living" document, and will be updated regularly to include up-to-date requirements and involve additional public safety stakeholders.

Next Steps….

- ❑ Perform a Gap Analysis
- ❑ Receive feedback from our target audience
- ❑ Establish a regular feedback mechanism from SoR stakeholders.
- ❑ Involve expanded stakeholders in the enhancement of the SoR
- ❑ Identify future architectures as technology grows

Acronym List

- **ACTD** Advanced Concept Technology Demonstration
- **AGILE** Advanced Generation of Interoperability for Law Enforcement
- **APCO** Association of Public-Safety Communications Officials – International
- **CapWIN** Capital Wireless Integrated Network
- **CIPSC** Coalition for Improved Public Safety Communications
- **DHS** Department of Homeland Security
- **DoD** Department of Defense
- **DOE** Department of Energy
- **DOI** Department of the Interior
- **DOJ** Department of Justice
- **DOT** Department of Transportation
- **FCC** Federal Communications Commission
- **FTE** Full Time Equivalent
- **HHS** Department of Health and Human Services
- **IACP** International Association of Chiefs of Police
- **IAFC** International Association of Fire Chiefs
- **IBET** Integrated Border Enforcement Teams
- **ISART** International Symposium on Advanced Radio Technologies
- **JTRS** Joint Tactical Radio System
- **MCC** Major City Chiefs
- **MCS** Major County Sheriffs
- **MOA** Memorandum of Agreement
- **MOU** Memorandum of Understanding
- **NACo** National Association of Counties
- **NASCIO** National Association of State Chief Information Officers
- **NCC** National Coordination Committee (within the FCC)
- **NCJA** National Criminal Justice Association
- **NCSL** National Conference of State Legislatures
- **NEMA** National Emergency Management Association
- **NFPA** National Fire Protection Association
- **NGA** National Governor's Association
- **NIJ** National Institute of Justice
- **NIST** National Institute of Standards and Technology
- **NLC** National League of Cities
- **NLECTC** National Law Enforcement and Corrections Technology Center
- **NPSTC** National Public Safety Telecommunications Council
- **NSA** National Sheriffs' Association
- **OLES** Office of Law Enforcement Standards
- **OMB** Office of Management and Budget
- **P25** Project 25
- **PMC** President's Management Council
- **PMO** Program Management Office
- **SDR** Software Defined Radio
- **S&T** Science and Technology
- **USCM** United States Conference of Mayors
- **USDA** United States Department of Agriculture

Contact Information

For more information on the SAFECOM Program, please contact:

- David Boyd, PhD
- Director, Program Management Office
- SAFECOM@dhs.gov

Or visit the SAFECOM website:

- www.safecomprogram.gov

- Background on public safety communications and interoperability
- Major challenges to interoperability
- Role, vision, and objectives of SAFECOM
- Public Safety Communications Statement of Requirements
- Appendixes

A: Spectrum

B: Funding

C: Standards

D: Security

Limited and fragmented radio spectrum contributes to public safety users inability to communicate

- Radio **spectrum** refers to the array of frequencies available for communications
- Most public safety agencies use spectrum to support both mission critical and day-to-day voice communications
- Spectrum is increasingly being used to support more advanced technologies such as—
  - Data
  - Imagery
  - Video transmissions
- The amount of spectrum available to the public safety community is insufficient to effectively carry out their critical missions
- Current public safety radio channels are located in many areas of the spectrum; however, no single radio or communications device can tune to all channels within the radio spectrum
- Other related barriers include—
  - Access to allocated spectrum (DTV transition)
  - Interference problems (800 MHz band)

In major disasters such as the Oklahoma City bombing, radio systems operated in different frequency bands, hindering communications interoperability

What is being done to ensure additional spectrum is available to public safety?

- The Balanced Budget Act of 1997 allocated 24 MHZ of spectrum to public safety
  - 764-776 MHz (TV channels 63 and 64)
  - 794-806 MHz (TV channels 68 and 69)
- Requires TV broadcasters to transition to new channels for digital television (DTV) broadcast by December 31, 2006

Federal Communications Commission

- Regulates interstate and international communications, including public safety spectrum
- Established an aggressive DTV implementation schedule to facilitate the availability of 700 MHz bands
- Proposing measures to streamline the authorization procedures for emerging technologies
- Established the National Coordination Committee (NCC) to—
  - Formulate an operational plan to achieve nationwide interoperability
  - Recommend interoperability digital modulation, trunking, receiving standards, and other technical matters that are common to public safety

NTIA

- Authorized the use of 20 frequencies between 162-174 MHz and 20 additional in the 406.1-420 MHz for mutual aid interoperability
  - Provides interoperability for joint local, state, and federal law enforcement operations,disasters, and emergencies

In 1996, the PSWAC Final Report made recommendations for public safety

PSWAC Subcommittee Findings/Recommendations Through 2010			
Spectrum	**Interoperability**	**Technology**	**Transition**
• Allocate portions of the 746–806 MHz, 4635-4685 MHz, and 5850-5925 MHz bands • Grant public safety access to unused spectrum adjacent to current operations	• Reduce total number of frequency bands • Establish new interoperability band below 512 MHz	• Develop technology to meet increasing data needs • Expect spectrum efficiency to improve • Observe digital technology as key for the future	• Develop plan for migration to a spectrum-efficient technology • Identify alternative funding mechanisms to transition to new technology or spectrum

Overall recommendations—

- Public safety services need 97.5 MHz of new spectrum by 2010
  - 25 MHz of general use spectrum is required in the near term
  - 2.5 MHz below 512 MHz dedicated for interoperability use is needed
- Appropriate use of commercial services should be encouraged
- System sharing at all levels of government should be promoted

Issues exist and must be addressed within frequency bands used by public safety

Frequency Band	Details	Issues
Below 512 MHz	• FCC required new public safety systems to transition to 12.5 KHz channels (from 25 KHz channels) to expand capacity and increase spectrum efficiency	• Purchase of new replacement equipment required by 2018 • Immediate interoperability hindered by preventing licensing and manufacturing of dual-mode equipment during transition
700 MHz	• The FCC designated channels 63, 64, 68, and 69 in the 764-806 band for public safety use • The FCC established the requirement that all 700 MHz transmissions must employ digital modulation	• Broadcast TV channels are currently operating in this spectrum • Freeing of spectrum is scheduled for 2007, but may be delayed • Equipment is still under development for 700 MHz band
800 MHz	• Public safety operations between 854.75 and 861 MHz experience harmful interference from commercial systems • Several plans, including the Consensus Plan have been proposed to solve the problem	• There is disagreement in public safety community over the most appropriate solution • There is no fast, inexpensive solution available and guaranteed
4.9 GHz	• The FCC allocated 50 MHz in the 4.9 GHz spectrum band to public safety • Licensing and technical rules for use were issued in April 2003 • Ideal band for short range, broadband communications	• Limited coverage area • New technology requires training, infrastructure, and standards, among others

Issues are being addressed at a regulatory level; however, they continue to plague agency operations

The current state of the 700 MHz frequency band...

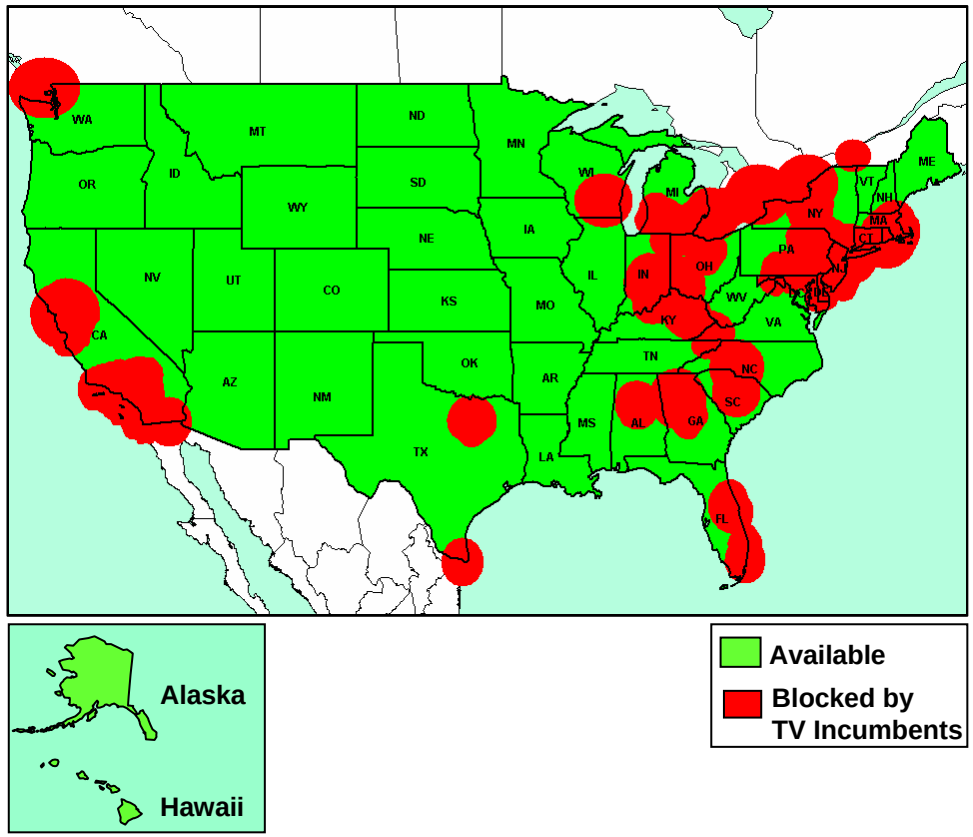
Background—

- The FCC designated TV channels 63, 64, 68, and 69 in the 746-806 MHz band for public safety use
  - Allocated 24 MHz at 764–776 MHz and 794–806 MHz for public safety
  - Allocated 36 MHz at 746–764 MHz and 776–794 MHz to be auctioned for commercial use (Auction 31 not scheduled)
  - Provided interference protection for TV broadcasters, low-power TV, and TV translator stations on channels 60–69 through December 31, 2006
- The FCC established the requirement that all 700 MHz transmissions must employ digital modulation

Key Challenges—

- Broadcast TV channels are currently operating in the 700 MHz public safety spectrum
- Freeing of this spectrum is scheduled for December 31, 2006, but may be delayed

700 MHz Public Safety Spectrum Availability



The current state of the 800 MHz frequency band…

Background—

- The 800 MHz band supports the operations of an array of diverse entities—
  - Public safety and public service providers
  - Specialized mobile radio (SMR) operations
  - Other business and industrial communications

Key Challenges—

- The various services using the 800 MHz band operate on interleaved channels
- This proximity of public safety channels to SMR channels (i.e., Nextel), increases the probability of interference and, consequently, hinders interoperability
- In March 2002, the FCC requested information on methods to resolve possible interference and received three major proposals offering mitigation strategies—

Consensus Parties

Motorola, Inc.

800 MHz Coalition

Consensus Parties

- "Consensus Plan" suggested restructuring the 800 MHz band
  - Consolidate frequencies by service type and eliminate cross-service interleaving
- Nextel to pay $700 million to relocate public safety operations

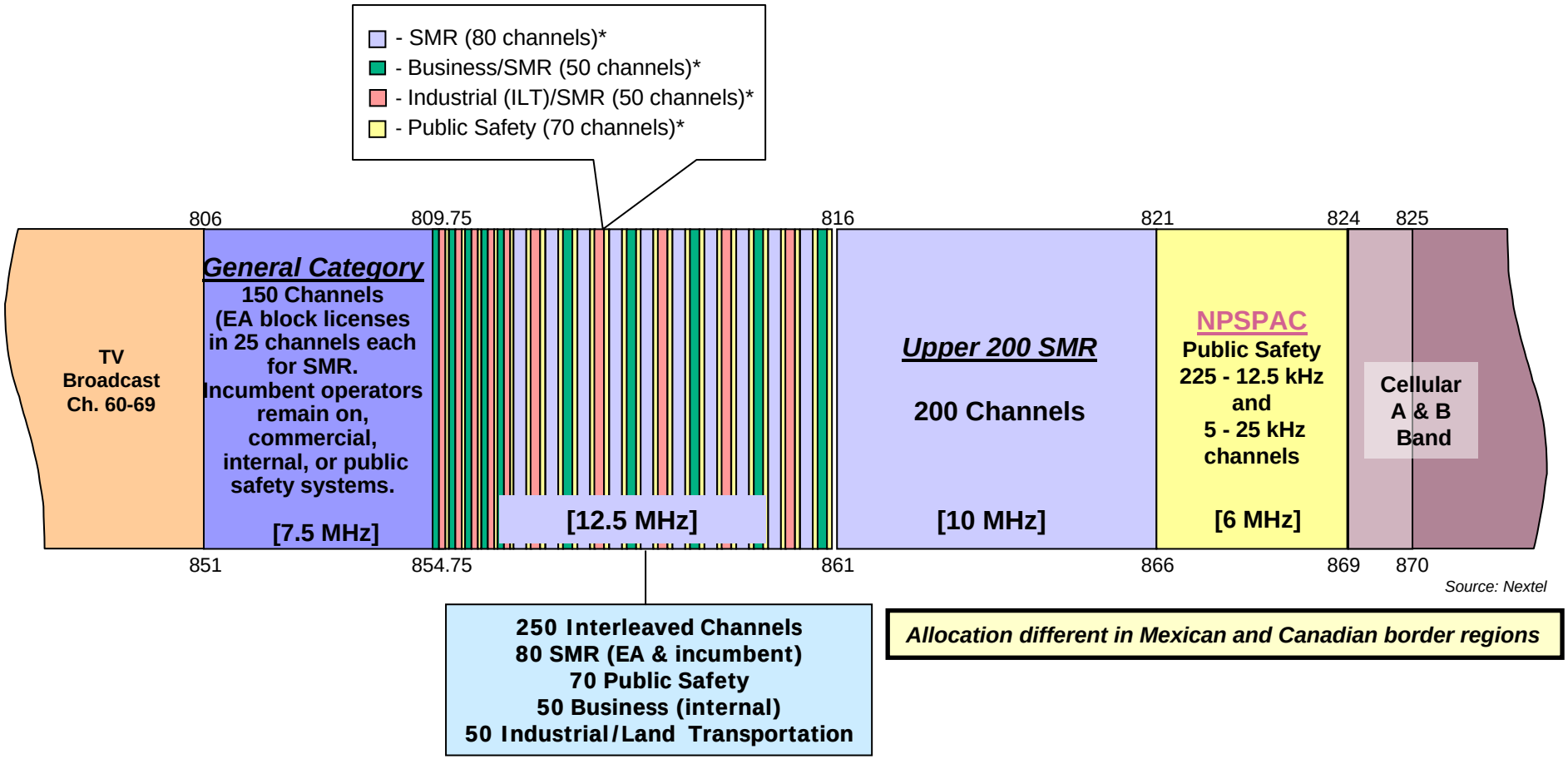
Motorola, Inc.

- Pointed to receiver improvements as an alternative to band reorganization
- Suggested that technology could dynamically adjust to the desired signal strength and reduce a receiver's acceptance of unwanted signals

800 MHz Coalition

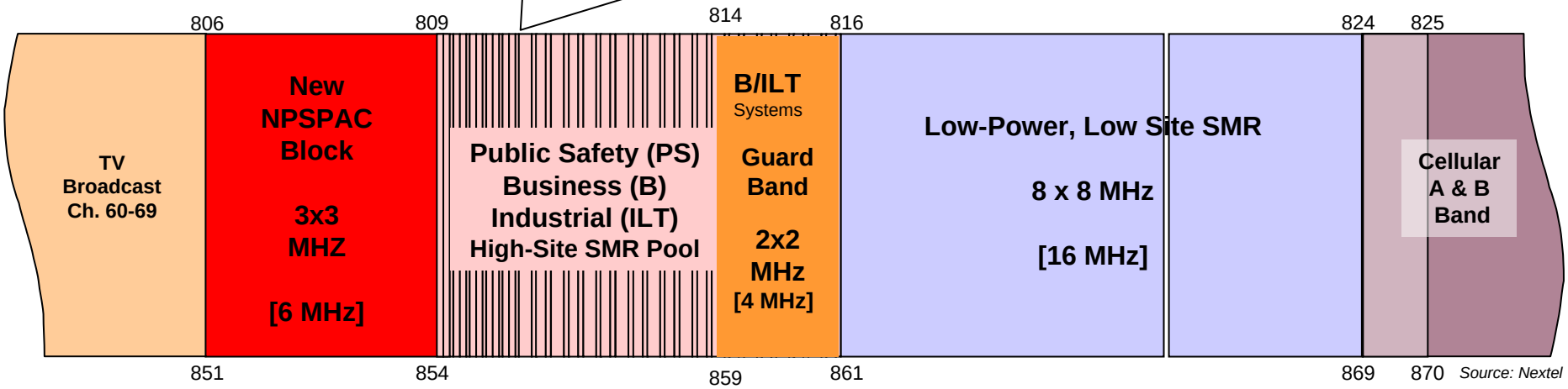
- "Balanced Approach" outlined a process to resolve interference through pre-planning and coordination
- Involved the adoption and codification of APCO's Best Practices, advanced receiver technology, and flexible license eligibility rules

Current 800 MHz FCC spectrum allocation…



Consensus Plan's suggested restructuring of the 800 MHz band…

- Public Safety Entities will have first access to new channels that were vacated by the relocated low-power, low-site SMR entities
- After 5 years of public safety relocation, B/ILT licensees will have access to this pool of available channels



Allocation different in Mexican and Canadian border regions

Additional allocations and spectrum related initiatives…

Refarming Below 512 MHz

Background—

- FCC released 2nd Report & Order 99-87 on February 25, 2003
- Within 6 months of publishing in the Federal Register—
  - No new systems with emissions greater than 12.5 kHz will be licensed for frequencies below 512 MHz
  - Modifications to systems will be prohibited if they extend the interference contours beyond what they are now licensed
  - Deadline for use of 25 KHz equipment in public safety market is January 1, 2018

Key Challenges—

- Purchase of new replacement equipment required by 2018
- Interoperability hindered by preventing licensing and manufacturing of dual-mode equipment during transition

4.9 GHz Band

Background—

- FCC allocated 50 MHz of spectrum from 4.94 to 4.99 GHz
- Permits public safety agencies to implement on-scene wireless networks for broadband operations including—
  - Streaming video
  - Rapid Internet and database access
  - Transfer of large files
- Gives every jurisdiction in the country access to spectrum for deployable, interoperable, broadband communications

Key Challenges—

- Limited coverage area
- New technology requires training, infrastructure, and standards, among others

What remains to be done?

Generally—

- ✓ Prioritize the resolution of all public safety interference so that lives and property are not unnecessarily put at risk

The public safety community can—

- ✓ Raise awareness among decision makers that an additional 23.5 MHz is still required to met all their existing and future telecommunications needs
- ✓ Pursue additional standards and cooperative measures to maximize interoperability in public safety spectrum

The FCC can—

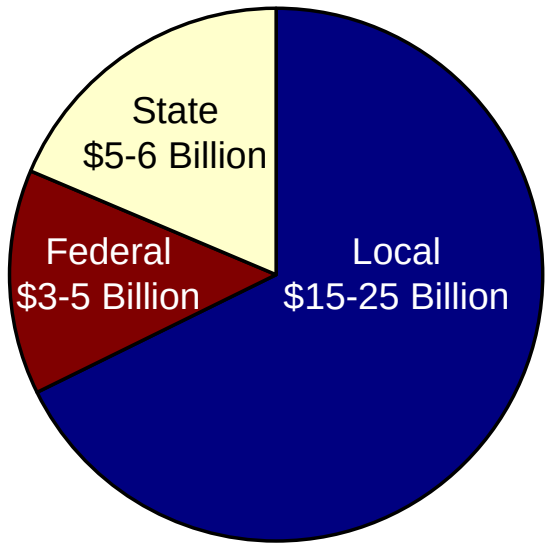
- ✓ Continue its aggressive actions in promoting the voluntary clearing of the 700 MHz band to accelerate the DTV transition
- ✓ Provide the additional public safety spectrum needed for interoperability below 512 MHz, voice communications, wideband data, and video applications

- Background on public safety communications and interoperability
- Major challenges to interoperability
- Role, vision, and objectives of SAFECOM
- Public Safety Communications Statement of Requirements
- Appendixes
  - A: Spectrum
  - B: Funding
  - C: Standards
  - D: Security

Funding has been cited as the primary obstacle to interoperability

- Between **$30–40 billion** in capital funding is required to address the aggregate local, state, and federal replacement requirement for radio systems
- Radio systems are often pitted against other public safety or community priorities (e.g., fire fighting equipment, school renovations)
  - Because existing systems are serviceable, radio networks often do not fare well in competition for limited government funding
- Operations and maintenance costs are high, increase as networks age, and must be paid on an ongoing basis
  - High annual recurring costs discourage the allocation of the capital dollars needed to upgrade or replace aging networks
- There is a lack of competition in the LMR marketplace, limiting the buying power of public safety agencies

Estimated System Replacement Costs Across Levels of Government



A funding strategy is needed to secure funding for wireless networking activities

Generic State and Local Wireless Network Funding Process

Estimating network lifecycle funding requirements	Developing a comprehensive funding strategy	Implementing the funding strategy	Maintaining full funding for the network lifecycle
• Identify network development alternatives • Establish a methodology to estimate network costs • Estimate the lifecycle costs of the network	• Review state and local funding mechanisms • Review federal funding mechanisms • Develop a funding strategy	• Develop a business case for a wireless network • Perform outreach communications and marketing • Develop partnerships • Request funding	• Measure network performance for continued support • Assess network funding requirements • Plan for the end of the network lifecycle

- Depending on the complexity and number of users, additional stages could be necessary
- A multidisciplinary, diverse team of skilled professionals is needed to support the funding process
- The public safety community must look at the long-term needs of a system when developing a funding strategy

Various types of government revenue and funding mechanisms are available to public safety

- Many funding mechanisms are available; however, few are dedicated specifically for public safety
- Federal mechanisms are usually tied to government or agency objectives
- State funds can target public safety needs and offer more flexibility than federal funding
- Localities receive federal and state funding, and also generate funding unique to their jurisdiction
  - Use of federal funds is often limited by guidelines and regulations
  - State government limits the use of mechanisms such as surcharges

Mechanisms for Funding Public Safety Radio Networks

Federal Level

Revenues
- Tax Revenue
- Surcharges
- Bonds and Notes

Funding Mechanisms
- Federal Appropriations
- Federal Asset Forfeiture Funds
- Off-Budget Trust Funds
- Grants and Cooperative Agreements

State Level

Revenues
- Intergovernmental Revenue
- State Taxes
- Surcharges
- User Fees
- Bonds

Funding Mechanisms
- State Appropriations
- State Grants
- State Trust Funds
- Investment and Capital Funds

Local Level

Revenues
- Intergovernmental Revenue
- Fees for Service
- Lease Revenue Bonds & Certificates of Participation

Funding Mechanisms
- Local General Fund Money
- Investment Funds
- Capital Improvement Funds

Funding for public safety systems is available through various federal sources

COPS

- Provides grants to state and local law enforcement to support community policing
- On February 20, 2003, President Bush signed a bill providing $584.1 million in 2003 appropriations for COPS
- $188.7 million is available through COPS Technology Grants and another $74.6 million is available through the Interoperable Communications Technology Program

ODP — Office for Domestic Preparedness

- Provides grants to enhance the capacity of state and local jurisdictions to respond to domestic terrorism incidents
- Received approximately $4 billion in grants for distribution in FY 04 that could be used for public safety including—
  - $1.7 billion for formula-based grants
  - $750 million for Firefighter Assistance Grants
  - $725 million for discretionary grants for high-threat, high-density urban areas
  - $500 million for law enforcement terrorism prevention grants
  - $40 million for Citizen Corps grants

NTIA — U.S. Department of Commerce, National Telecommunications & Information Administration

- Supports the Technology Opportunities Program (TOP), which provides grants for model projects demonstrating innovative uses of telecommunications and information technologies
- In FY 03, TOP grants were distributed to local, state, and tribal government in 22 states

What remains to be done?

Generally—

✓ Continue to increase funding levels and identify new mechanisms to distribute the funds

Public safety agencies can—

✓ Develop and target training and education programs to help make the best use of existing funding mechanisms and assist with the development of funding proposals and spending plans

- Public safety officials need to become more knowledgeable of available funding sources and how to appropriately engage in the funding process

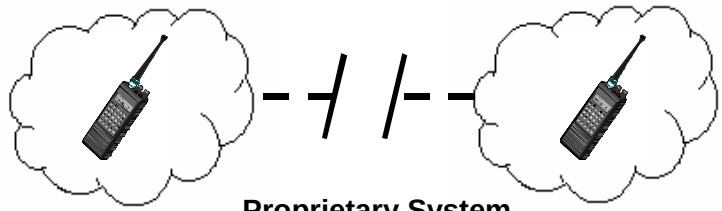
✓ Establish system lifecycle strategies that take advantage of proven cost-reduction methods

- Develop public–private partnerships, shared infrastructure, and cooperative procurement processes

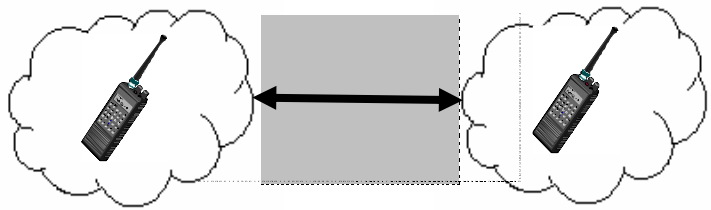
- Background on public safety communications and interoperability
- Major challenges to interoperability
- Role, vision, and objectives of SAFECOM
- Public Safety Communications Statement of Requirements
- Appendixes
  - A: Spectrum
  - B: Funding
  - C: Standards
  - D: Security

The lack of open standards has hindered public safety interoperability

- **Standards** are guidelines that all equipment operating in a given frequency must follow
- The need for open standards became urgent about 20 years ago
  - Manufacturers began making improvements to enhance the functionality and efficiency of their systems
- Each manufacturer uses unique and proprietary signaling protocols and encryption methods
- These proprietary protocols cause incompatibility among different radio systems built by different manufacturers
- Manufacturers argue that obtaining licenses for intellectual property rights (IPRs) contained in most standards makes compliance too expensive
- Public safety officials are forced to purchase all of their equipment from one manufacturer, limiting the buying power of public safety agencies



Proprietary System



Standards-Based System

Public safety communications is often hampered by the use of multiple proprietary protocols

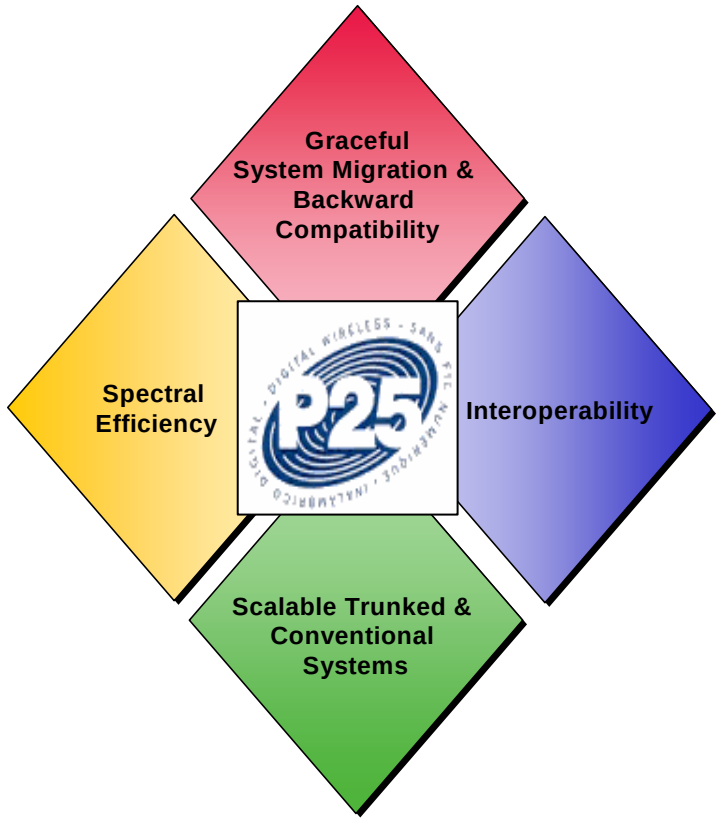
The history of public safety communications standards development…

Conventional FM Analog Technology	Current Standards	Future Standards
• Communications technology is inefficient and outdated • Implementation of new technologies has created proprietary protocols	• Standards are being developed by the public safety community in cooperation with vendors • Standards are not complete, delaying widespread adoption and limiting large metropolitan areas to a single vendor	• Goal: Open standard for voice and data technologies • Private industry standards will be leveraged • Standards will ensure necessary functionality, security, and system performance with cost efficiency

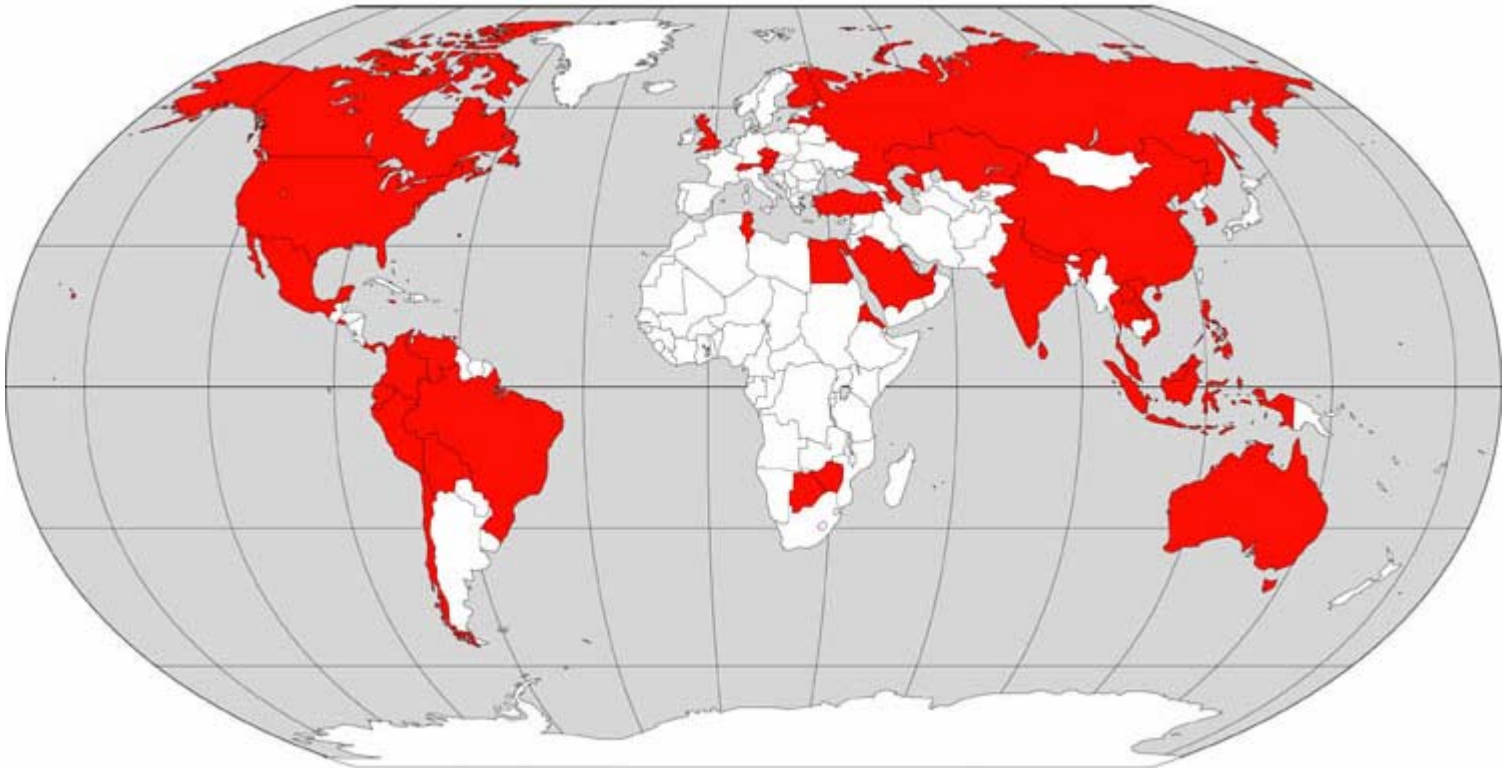
In general, the public safety has lacked sufficient resources to support broad, vigorous, ongoing participation in standards development

Project 25's importance to public safety interoperability…

- Founded by the Association of Public Safety Communications Officials (APCO) and the Association for Telecommunications and Technology Professionals Serving State Government (NASTD)
- Developing a suite of technical specifications for digital, land mobile radio communications systems
- P25 standards are designed to be backward compatible to analog FM
- Enable interoperability through open standards, which eliminate proprietary protocols
- Allows for increased selection of trunked and conventional infrastructure components
  - Promotes competition among manufacturers, potentially lowering the price for equipment
- Endorses spectrally efficient technologies
- Phase 1 standards specify—
  - How voice sound waves are converted into digital format
  - How subscriber units and infrastructure components communicate with each other
- Phase 2 is working to further develop standards for fixed-station interference and console interface



Many countries have implemented P25 interoperable equipment or networks



Australia	Canada	El Salvador	Kazakhstan	Peru	Trinidad
Austria	Chile	Eritrea	Korea	Philippines	Tunisia
Azerbaijan	China	Finland	Kuwait	Russia	Turkey
Bahrain	Colombia	India	Latvia	Saudi Arabia	United Kingdom
Bermuda	Costa Rica	Indonesia	Laos	Singapore	USA
Botswana	Czech Republic	Hong Kong Special	Malaysia	Slovenia	United Arab Emirates
Brazil	Ecuador	Administrative Region, China	Mexico	Sri Lanka	Venezuela
Brunei	Egypt	Jamaica	Nepal	Switzerland	Vietnam
				Thailand	Zimbabwe

Project MESA is working to improve interoperability

- Is a joint project of the Telecommunications Industry Association (TIA) and the European Telecommunications Standards Institute (ETSI)
- Works to develop international standards for the next generation of public safety and emergency communications
- Project MESA is planned to bring cross-border interoperability for coordinating responses to natural disasters and other emergency situations
- Envisions an on-site, independent network deployed that provides voice and data capabilities to all public safety officials
- Initial Statement of Requirements (SOR) was approved in 2002 by the Project MESA Steering Committee
- SOR defines future user requirements to involve 2 Mbps data rates or greater to offer varying applications, which include—
  - Secure and interoperable information
  - Analog/digital voice and video
  - High-speed data
  - Still photographs
  - Enhanced patient and response worker bio-telemetry
- MESA Technical System Specifications Group and its subgroups have begun work on the technical specifications

What remains to be done?

Generally—

- ✓ Continue to coordinate standards development within the public safety community to ensure a standards that meets the needs of public safety

- ✓ Develop additional open standards for the very high frequency (VHF) band
  - – The majority of state and local agencies and nearly all federal agencies continue to operate in this frequency band

The public safety community can—

- ✓ Continue to seek resources to ensure participation in standards development processes

Industry can—

- ✓ Design and manufacture standards-compliant radio infrastructure for the public safety community

The FCC can—

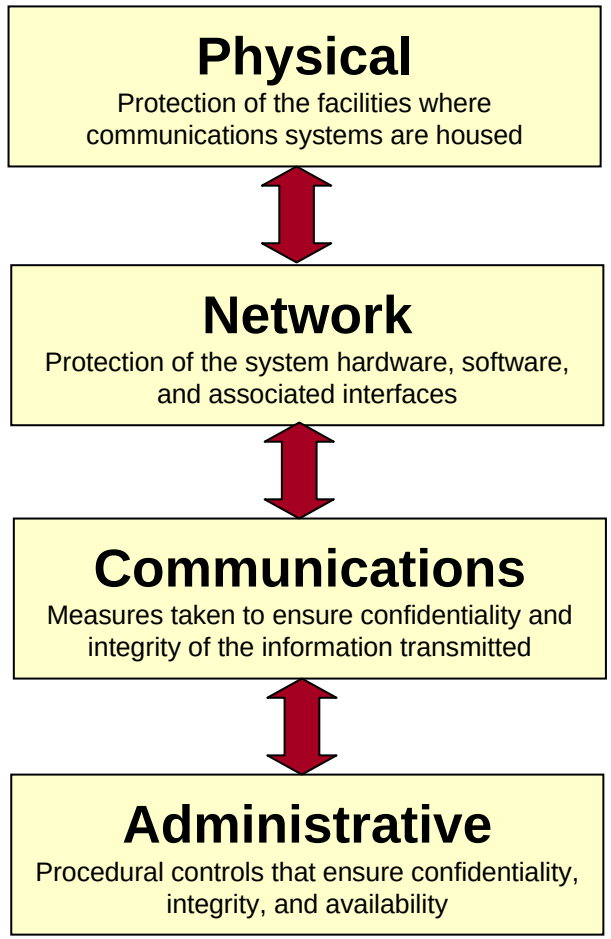
- ✓ Stress backward compatibility to maintain interoperability as local, state, and federal public safety agencies replace their current communications systems
  - – The deadline for prohibiting certification of equipment that supports 25 kHz channels is January 1, 2005, which has halted the development of P25-compliant radio equipment

- Background on public safety communications and interoperability
- Major challenges to interoperability
- Role, vision, and objectives of SAFECOM
- Public Safety Communications Statement of Requirements
- Appendixes
  - A: Spectrum
  - B: Funding
  - C: Standards
  - D: Security

For years, public safety has contended with security risks to their communications systems

- Communications system security is the process of developing and implementing specific plans, policies, and procedures to secure public safety communications
- Communications are generally not safe from sophisticated criminals attempting to intercept information traveling over the air
- Public safety agencies are facing an ever-increasing number of threats—
  - Coordinated terrorists attacks to physical communications infrastructure
  - Remote attacks to computer-based systems
- Network-related security vulnerabilities based on digital, computer-based technology add to the array of traditional threats
- The evolution toward automated, computer-controlled communications systems makes the threat of a system hacker more critcal
- Public safety agencies are not adequately incorporating security mechanisms or coutermeasures into their systems due to limited awareness and funding limitations

Communications security encompasses these interrelated components—



The threats to public safety communications are readily available and in use

In Ohio, burglars used scanners to monitor police communications, break into a home, and plan their escape just before officers arrived

***RISK*: Communications "in the clear" are being monitored by criminals and can be used to counter public safety responses**

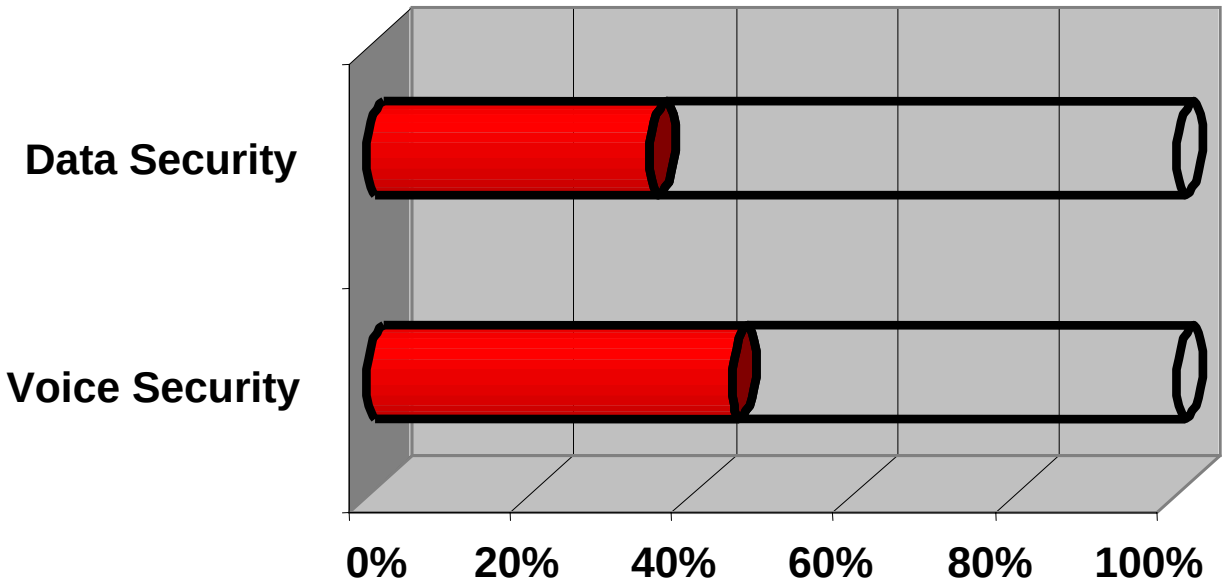
In Massachusetts, an attack on the telephone system at the Worchester Airport caused a communications outage and affected all interconnected systems, including the radio system

***RISK*: Interconnected systems can be more vulnerable without proper protection because when one part of the system is compromised, the rest of the system can be affected**

In Scott County, Iowa, vandals severed a 295-foot tower using a hacksaw—the fallen tower caused a loss of communications in half the county until alternate arrangements could be made

***RISK*: Unprotected communications equipment is vulnerable to vandalism and terrorism that may cause large-scale communications outages**

Most law enforcement agencies do not employ voice or date security protection to counter threats



- Thirty-five percent of responding law enforcement agencies use data security protection*
- Forty-five percent of responding law enforcement agencies use voice security protection*

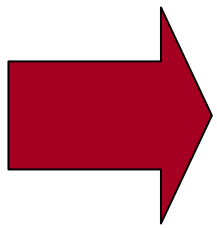
Source: NIJ Research Report: *State and Local Law Enforcement Wireless Communications and Interoperability: A Quantitative Analysis*

* Based on a sample size of 1,334 agencies

As public safety communications systems evolve, security issues and threats proliferate

CHALLENGES

- Greater interconnectivity causing an increase in system "entry points"
- Interoperability among all levels of government
- Increased network data transfer
- Unspecified security requirements
- Increased sophistication of "bad guys"
- Increased public safety information availability to public
- Storage of critical radio resources on computer-based systems
- Increased encryption use
- Proper inventory control of radio equipment



THREATS

- Interception of unencrypted sensitive network traffic
- Unauthorized people masquerading as system users
- Malicious people disabling radio subscribers
- Re-mapping talk groups to different channels
- Transmission of false information over the system
- Inadvertent release of sensitive information
- Password guessing and random dial-in modem attacks
- Improper encryption and system key management

What is being done to enhance communications security for public safety?

- The Federal Government has recognized the need to safeguard critical nationwide infrastructures
  - Emergency services (i.e., law enforcement, fire, and EMS) is considered one of the Nation's most critical infrastructures

- National-level policies have been set forth to address security problems of public safety communications systems
  - Executive Order 13010 (July 1996) stresses the need to protect critical infrastructures from physical, electronic, radio frequency, and computer attacks
  - Presidential Decision Directive (PDD) 63 (May 1998) states that addressing these vulnerabilities would require flexible, evolutionary, and coordinated approaches that span both the public and private sectors
  - Classified PDD 67 (October 1998) deals with the continuity of government operations
  - The SAFECOM Resource Center has developed a number of documents to help guide public safety officials through security issues including—
    - Public Safety Communications Security Briefing – Provides an overview of the security challenges facing public safety communications systems and discusses near- and long-term solutions
    - LMR System Recommended Security Policy – Presents a template to guide the development of security policies for public safety wireless systems
    - Key Management Plan Template – Provides a template to help guide the development of encryption key management plans

What remains to be done?

Generally—

- ✓ Coordinate among leaders from all levels of the government and public safety officials to create security solutions
- ✓ Standards associations, vendors, and the public safety community must work together and adopt overarching security standards, procedures, and guidelines

Government leaders can—

- ✓ Understand the potential security threats and risks associated with evolving public safety communications systems

Public safety agencies can—

- ✓ Incorporate security measures into their existing systems to the greatest extent possible
- ✓ Include security specifications as part of their request for proposals when pursuing a new system implementation

Equipment manufacturers and system integrators can—

- ✓ Incorporate public safety needs into their products and service offerings